May 2021

'Care Share

Awareness is the Key to Phishing and Spoofing

Just like with regular fishing, when phishing the criminals are baiting a hook to catch you. **Phishing is a technique of sending an email intending to trick you** into clicking on a malicious link or downloading an attachment potentially laced with malware.

The scammer may use spoofing to accomplish this. **Spoofing is the act of disguising a communication from an unknown source as being from a known, trusted source.** This can be done through email, texts, the mail, or the phone, often just by changing one letter, symbol, or number—to convince you that you are interacting with a trusted source.

On the phone, the caller might impersonate Medicare or another organization to collect your personal information. This includes deliberately falsifying information shown on your caller ID display to disguise their identity. It is very easy to use technology to even make it look like a call is coming from a local number when in fact they are in a different country.

Another variation is through text messages. Phishing emails and texts are easy, cheap, and effective. Criminals have three primary ways they steal information: 1) malicious web links, 2) malicious attachments, and 3) fraudulent data-entry forms. They throw out thousands at a time but only need to hook a few. Don't get hooked!

Phishing often tells a story to trick you into responding in some way. They may

- say they've noticed some suspicious activity or log-in attempts
- claim there's a problem with your account or your payment information
- say you must confirm some personal information
- include a fake invoice
- want you to click on a link to make a payment
- say you're eligible to register for a government refund
- offer a coupon for free stuff
- direct you to a website to fill out a survey or assessment

Phishing is considered social engineering because the methods they use, such as forgery, misdirection and lying, manipulates human psychology and encourages us to act before we think things through. **Use caution if you are being pressured for personal information** or asked to make a quick decision.

Montana SMP is a program coordinated by Missoula Aging Services and partnered with local Area Agencies on Aging. This project was supported by grant #90MPPG0052 from the U.S. Administration for Community Living, Department of Health and Human Services, Washington D.C., 20201. Points of view or opinions do not necessarily represent official ACL policy.

So aside from moving to a deserted island, what can you do?

You may not be able to tell right away if a mailing, call, email, or text is legitimate. **Be extremely careful about responding to any request for personal identifying information**. Never give out personal information such as account numbers, Medicare or Social Security numbers, mother's maiden name, passwords, or other identifying information in response to unexpected calls or if you are the least bit suspicious.

The best advice is to stop answering calls from unknown numbers. If you have voicemail set up, use it. Once you pick up the call it marks you as having a live line, so even if you hang up, they know you are a live person, and this will keep you on their call rotation.

If you answer the phone and the caller - or a recording - asks you to hit a button to stop getting the calls, just hang up.

Do not respond to any questions, especially those that can be answered with "Yes" or "No."

Regarding emails and texts, do not click on links. Malicious links will take users to impostor websites or to sites infected with malicious software, also known as malware. Malicious links can be disguised to look like trusted links and are embedded in logos and other images.

If you get a pop-up message to call tech support, ignore it. Some pop-up messages about computer issues are legitimate, but do not call a number or click on a link that appears in a pop-up message warning you of a computer problem.

Do not open invoices or other attachments without checking the source first. These look like legitimate file attachments but are infected with malware that can compromise computers.

Lastly, beware of fraudulent data entry forms including assessments or surveys that ask you to fill in sensitive information—such as user IDs, passwords, credit card data, and phone numbers.

In general, if you get any type of inquiry from anyone who says they represent a company or a government agency and are wanting to collect your personal information, **separately look up the phone number on your account statement, in the phone book, or on the company's or government agency's website to verify the authenticity of the request.**

If you think you've been the victim of phishing or spoofing and have given out personal information, you can report identity theft, and get help with a recovery plan, at the Federal Trade Commission's IdentityTheft.gov site. You can also **call the FTC at 877-438-4338.**

If you have given out your Medicare number and think you have been the victim of medical identity theft, call your local Montana SMP at 1-800-551-3191.

The Senior Medicare Patrol (SMP) helps to educate Medicare beneficiaries about ways to prevent, detect, and combat Medicare fraud. For more information about Medicare fraud, visit the Stop Medicare Fraud website at www.stopmedicarefraud.org.